le: 4410-NW

DEPARTMENT OF JUSTICE

[CPCLO Order No. 002-2021]

Privacy Act of 1974; Systems of Records

AGENCY: United States Department of Justice.

ACTION: Notice of a Modified System of Records.

SUMMARY: Pursuant to the Privacy Act of 1974, 5 U.S.C. 552a, and Office of Management and Budget (OMB) Circular No. A-108, notice is hereby given that the Department of Justice (Department or DOJ), proposes to modify an existing DOJ system of records previously titled, "Department of Justice Computer Systems Activity and Access Records," JUSTICE/DOJ-002. The Department proposes to modify JUSTICE/DOJ-002 to reflect changes in technology, including the increased ability of the Department to link individuals to information technology, information system, or network activity, and to better describe the Department's records linking individuals to reported cybersecurity incidents or their access to certain DOJ information technologies, information systems, and networks through the Internet or other authorized connections.

DATES: In accordance with 5 U.S.C. 552a(e)(4) and (11), this notice is effective upon publication, subject to a 30-day period in which to comment on the routine uses, described below. Please submit any comments by **[INSERT DATE 30 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER]**.

ADDRESSES: The public, Office of Management and Budget (OMB), and Congress are invited to submit any comments by mail to the Department of Justice, ATTN: Privacy Analyst, Office of Privacy and Civil Liberties, 145 N St. NE, Suite 8W.300, Washington, DC 20530, by facsimile at 202-307-0693, or by email to *privacy.compliance@usdoj.gov*.

FOR FURTHER INFORMATION CONTACT: Nickolous Ward, DOJ Chief Information Security Officer, (202) 514–3101, 145 N Street NE, Washington, DC 20530.

SUPPLEMENTARY INFORMATION:

In accordance with the Federal Information Security Modernization Act of 2014, among other authorities, DOJ is responsible for complying with information security policies and procedures requiring information security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of DOJ information and information systems. *See, e.g.*, 44 U.S.C. 3554 (2018). Consistent with these requirements, DOJ must ensure that it maintains accurate audit and activity records of the observable occurrences on its information systems and networks (also referred to as "events") that are significant and relevant to the security of DOJ information and information systems. These audit and activity records may include, but are not limited to, information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

Additionally, monitored events—whether detected utilizing information systems maintaining audit and activity records, reported to the Department by information system users, or reported to the Department by the cybersecurity research community and members of the general public conducting good faith vulnerability discovery activities—may constitute occurrences that (1) actually or imminently jeopardize, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitute a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. The Department has developed a formal process to track and document these reported "incidents," which may, in limited circumstances, include records of individuals reporting, or otherwise associated with, an actual or suspected event or incident.

The system of records previously titled JUSTICE/DOJ-002, "Computer Systems Activity and Access Records," covers the Department's tracking of all DOJ information technology, information system, and/or network activity, including any access, whether authorized or unauthorized, by users to any DOJ information technology, DOJ information systems, and/or DOJ networks. These records assist Department information security professionals in protecting DOJ data, ensuring the secure operation of DOJ information systems, and tracking and documenting incidents reported to the Department. JUSTICE/DOJ-002 was first published at 64 FR 73,585, on December 30, 1999, and later modified at 66 FR 8,425, on January 31, 2001, and 82 FR 24,147, on May 25, 2017. The revisions to this notice reflect advances in technology, such as the ability of authorized users to connect to Department information systems through the Internet or other authorized network connections, as well as the increased ability of the Department to link the identity of individuals or subjects associated with an actual or suspected event or incident for security and administrative purposes.

The Department proposes to modify JUSTICE/DOJ-002 by: revising the title of the system of records to, "Department of Justice Information Technology, Information System, and Network Activity and Access Records;" modifying and clarifying the location of the system's records; clarifying the individuals covered by the system to include any and all individuals who access Department information systems for any reason and from any location; clarifying the way in which the records maintained in this system of records are retrieved; expanding the routine uses of records for disclosures that are functionally equivalent to the purpose for which the DOJ information is collected, or that are necessary and proper uses of the DOJ information, to enhance the flexibility of JUSTICE/DOJ-002; and to notify the public that the Department intends to claim certain Privacy Act exemptions, promulgated elsewhere in the Federal Register. DOJ is republishing the entire system of records notice for ease of reference to these changes.

In accordance with Privacy Act requirements of 5 U.S.C. 552a(r), the Department has provided a report to OMB and to Congress on this revised system of records.

Dated: July 1, 2021.

Peter A. Winn,

Acting Chief Privacy and Civil Liberties Officer,

United States Department of Justice.

JUSTICE/DOJ-002

SYSTEM NAME AND NUMBER:

Department of Justice Information Technology, Information System, and Network Activity and Access Records, JUSTICE/DOJ-002.

SECURITY CLASSIFICATION:

Unclassified, Controlled Unclassified Information, and Classified records.

SYSTEM LOCATION:

Records will be maintained electronically at Department of Justice offices, other sites utilized by the Department of Justice, and in information technology, information systems, or networks owned, operated by, or operated on behalf of the Department of Justice. Most records will be maintained electronically at one or more of the Department's Core Enterprise Facilities (CEF), including, but not limited to: CEF East, Clarksburg, WV 26306; CEF West, Pocatello, ID 83201; or CEF-DC, Sterling, VA 20164. Records may also be maintained at the individual information technology or end point of activity within the DOJ network, and may be located locally on the physical information technology or end point before being consolidated and stored for analysis and investigation.

Records within this system of records may be transferred to a Department-authorized cloud service provider, where records would be limited to locations within the Continental United States. Access to these electronic records includes all locations at which DOJ System Managers operate or are supported, including but not limited to the Robert F. Kennedy Department of Justice Building, 950 Pennsylvania Avenue N.W., Washington, DC 20530. Some or all system information may also be duplicated at other locations where the Department has granted direct access to support DOJ System Manager operations, system backup, emergency preparedness, and/or continuity of operations. To determine the location of particular records maintained in this system of

records, contact the system manager using the contact information listed in the "SYSTEM MANAGER(S)" paragraph, below.

SYSTEM MANAGER(S):

DOJ Chief Information Security Officer, (202) 514–3101, 145 N Street NE, Washington, DC 20530.

The Department has delegated to component-level Chief Information Officers and Chief Information Security Officers, subject to the oversight of the DOJ Chief Information Officer and/or DOJ Chief Information Security Officer, certain responsibilities for maintaining DOJ information technology, information system, and network activity and access records. Processes and procedures detailed in this system of records notice may be implemented by component-level Chief Information Officers and/or Chief Information Security Officers, at the direction of the DOJ Chief Information Officer and/or DOJ Chief Information Security Officer. Correspondence and/or requests from individuals may be referred to the appropriately delegated component-level Chief Information Officer and/or Chief Information Security Officer.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

The Federal Information Security Modernization Act of 2014, 44 USC 3551 *et seq*.; Executive Order No. 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information (2011); Executive Order No. 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (2017); OMB Circular A-130, Managing Information as a Strategic Resource (2016); OMB Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information (Jan. 3, 2017); OMB Memorandum M-20-32, Improving Vulnerability Identification, Management, and Remediation (Sept. 2, 2020).

PURPOSE(S) OF THE SYSTEM:

The purpose of this system of records is to ensure that the Department can track information system access and implement information security protections commensurate with the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of DOJ information and information systems. Records in this system of records are used by system administrators and security personnel, or persons authorized to assist these personnel, for the purpose of: reviewing and analyzing DOJ information and DOJ information system activity and access events for indications of inappropriate, unusual, or abnormal activity; tracking, documenting, and handling cybersecurity events and incidents; drafting, reviewing, and revising DOJ audit and accountability policies; supporting audit reviews, analyses, reporting requirements, and after-the-fact investigations of events; planning and managing system services; and otherwise performing their official duties. Authorized DOJ personnel may use the records in this system for the purpose of investigating improper access or other improper activity related to information system access; initiating disciplinary or other such action; or, where the record(s) may appear to indicate a violation or potential violation of the law, referring such record(s) to the appropriate investigative arm of DOJ, or other law enforcement agency for investigation.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

The categories of individuals covered by this system encompass all individuals who are provided DOJ information technology, access DOJ information systems, or transmit information across the DOJ network. This includes: individuals who use authorized DOJ information technology, information systems, and/or networks to send or receive DOJ information or DOJ-related communications, access Internet sites, or access any DOJ information technologies, information systems, or DOJ information; individuals from outside DOJ who communicate electronically with DOJ users, DOJ information technologies, DOJ information systems, and/or DOJ networks; individuals reporting,

tracking, documenting and/or otherwise associated with cybersecurity incident and/or event activities; and any individuals who attempt to access DOJ information technologies, DOJ information systems, and/or DOJ networks, with or without authorization.

CATEGORIES OF RECORDS IN THE SYSTEM:

Records in this system of records may include:

A. Access and activity logs that establish the types of events that occurred on an information system; when the events occurred; where the events occurred; the source of the events; the outcome of the events; and the identity of any individuals or subjects associated with the events. Such information includes, but is not limited to: time stamps recording the data and time of access or activity; source and destination addresses; user, device, and process identifiers, including Internet Protocol (IP) address, Media Access Control (MAC) address, and event descriptions; success/fail indications; filenames involved; full text recording of privileged commands; and/or access control or flow control rules invoked. Such information may be collected and aggregated by the operating system or application software locally within an information technology, information system, or network.

B. Information relating to any individuals accessing DOJ information, DOJ information technologies, DOJ information systems, or DOJ networks, including but not limited to: records contained within JUSTICE/DOJ-020 DOJ Identity, Credential, and Access Service Records System, 84 FR 60110 (Nov. 7, 2019); user names; persistent identifiers (such as a User ID); contact information, such as title, office, component, and agency; and the authorization of an individual's access to systems, files, or applications, such as signed consent forms or Rules of Behavior forms, or access authentication information (including but not limited to passwords, challenge questions/answers used to confirm/validate a user's identity, and other authentication factors).

C. Records on the use of electronic mail, instant messaging, other chat services, electronic call detail information (including name, originating/receiving numbers, duration, and date/time of call), and electronic voicemail.

D. Records of Internet access from any information technology connected to a DOJ information system, on a DOJ network, or through authorized connections to DOJ networks and DOJ information systems, including the IP address of the information technology being used to initiate the Internet connection and the information accessed.

E. Audit reviews, analyses, and reporting, including but not limited to, audits that result from monitoring of account usage, remote access, wireless connectivity, mobile device connection, configuration settings, system component inventory, physical access, and communications at the information system boundaries.

F. Actual or suspected incident or event report information, including but not limited to: information related to individuals reporting, tracking, documenting and/or otherwise associated with a cybersecurity incident and/or event; information related to reporting, tracking, investigating, and/or addressing an incident or event (e.g., data/time of the incident or event; location of incident or event; type of incident or event; storage medium information; safeguard information; external/internal entity report tracking; data elements associated with the incident or event; information on individuals impacted; information on information system(s) impacted; remediation, response, or notification actions; lessons learned; risk of harm and compliance assessments); and information related to discovering, testing, reporting, tracking, investigating, and/or addressing a security vulnerability or indicator of a security vulnerability.

RECORD SOURCE CATEGORIES:

Records covered by this system of records are generated internally (i.e., information technology, information system, and/or network activity logs) regardless of the location from which an individual accesses DOJ information or DOJ information

systems, manually sourced from DOJ personnel, or sourced directly from the individual on whom the record pertains.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system of records may be disclosed outside the Department as a routine use pursuant to 5 U.S.C. 552a(b)(3) under the circumstances or for the purposes described below, to the extent such disclosures are compatible with the purposes for which the information was collected:

A. To an organization or individual in both the public or private sector where there is reason to believe the recipient is or could become the target of a particular criminal activity or conspiracy or other threat, to the extent the information is relevant to the protection of life, health, or property. Information may be similarly disclosed to other recipients who share the same interests as the target or who may be able to assist in protecting against or responding to the activity or conspiracy.

B. To appropriate officials and employees of a federal agency for which the Department is authorized to provide a service, when disclosed in accordance with an interagency agreement and when necessary to accomplish an agency function articulated in the interagency agreement.

C. To any person(s) or appropriate Federal, state, local, territorial, tribal, or foreign law enforcement authority authorized to assist in an approved investigation of or relating to the improper usage of DOJ information technologies, DOJ information systems, and/or DOJ networks.

D. To any criminal, civil, or regulatory law enforcement authority (whether Federal, state, local, territorial, tribal, or foreign) where the information is relevant to the recipient entity's law enforcement responsibilities.

E. To a governmental entity lawfully engaged in collecting law enforcement, law enforcement intelligence, or national security intelligence information for such purposes.

F. To any person, organization, or governmental entity in order to notify them of a serious terrorist threat for the purpose of guarding against or responding to such a threat.

G. To Federal, state, local, territorial, tribal, foreign, or international licensing agencies or associations which require information concerning the suitability or eligibility of an individual for a license or permit.

H. Where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate Federal, state, local, territorial, tribal, or foreign law enforcement authority or other appropriate entity charged with the responsibility for investigating or prosecuting such violation or charged with enforcing or implementing such law.

I. To complainants and/or victims to the extent necessary to provide such persons with information and explanations concerning the progress and/or results of the investigation or case arising from the matters of which they complained and/or of which they were a victim.

J. To any person or entity that the Department has reason to believe possesses information regarding a matter within the jurisdiction of the Department, to the extent deemed to be necessary by the Department in order to elicit such information or cooperation from the recipient for use in the performance of an authorized activity.

K. In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body, when the Department of Justice determines that the records are

arguably relevant to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

L. To an actual or potential party to litigation or the party's authorized representative for the purpose of negotiation or discussion of such matters as settlement, plea bargaining, or in informal discovery proceedings.

M. To the news media and the public, including disclosures pursuant to 28 CFR § 50.2, unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

N. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, interagency agreement, or other assignment for the Federal government, when necessary to accomplish an agency function related to this system of records.

O. To designated officers and employees of state, local, territorial, or tribal law enforcement or detention agencies in connection with the hiring or continued employment of an employee or contractor, where the employee or contractor would occupy or occupies a position of public trust as a law enforcement officer or detention officer having direct contact with the public or with prisoners or detainees, to the extent that the information is relevant and necessary to the recipient agency's decision.

P. To appropriate officials and employees of a federal agency or entity that requires information relevant to a decision concerning the hiring, appointment, or retention of an employee; the issuance, renewal, suspension, or revocation of a security clearance; the execution of a security or suitability investigation; the letting of a contract; or the issuance of a grant or benefit.

Q. To a former employee of the Department for purposes of: responding to an official inquiry by a federal, state, or local government entity or professional licensing

authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

R. To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

S. To the National Archives and Records Administration for purposes of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

T. To appropriate agencies, entities, and persons when: (1) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

U. To another Federal agency or entity, when the Department determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

V. To any agency, organization, or individual for the purpose of performing authorized audit or oversight operations of DOJ, and meeting related reporting requirements.

W. To such recipients and under such circumstances and procedures as are mandated by federal statute or treaty.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Records in this system of records are stored on paper and/or in electronic form. Records are stored securely in accordance with applicable Executive Orders, statutes, and agency implementing recommendations.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records are collected in real time from all DOJ information technologies and endpoints on the DOJ network and aggregated in databases searchable by identifying characteristics, including, but not limited to, name, user ID, email address, or IP address. Records may be retrieved as part of routine network and information system security monitoring, cybersecurity incident response, database activity monitoring, or in support of other administrative or security investigations in accordance with appropriate laws, rules, and policies.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records of verification, authorization, access, and other activities generated by DOJ information technologies, DOJ information systems, and/or DOJ networks shall be retained in accordance with applicable records schedules, including but not limited to General Records Schedule 3.1 and 3.2. After the appropriate retention period, records will be destroyed/deleted, in accordance with appropriate media sanitization procedures.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Information in this system is safeguarded in accordance with appropriate laws, rules, and policies, including the Department's automated systems security and access policies. Access to such information is limited to Department personnel, contractors, and other personnel who have an official need for access in order to perform their duties. Records are maintained in an access-controlled area, with direct access permitted to only authorized personnel. Electronic records are accessed only by authorized personnel with accounts on the Department's network. Additionally, direct access to certain information may be restricted depending on a user's role and responsibility within the organization and system. Paper records are safeguarded in accordance with appropriate laws, rules, and policies.

RECORD ACCESS PROCEDURES:

A request for access to a record from this system of records must be submitted in writing and comply with 28 CFR Part 16, and should be sent by mail to the Justice Management Division, ATTN: FOIA Contact, Room 1111, Robert F. Kennedy Department of Justice Building, 950 Pennsylvania Avenue, N.W., Washington, DC 20530-0001, or by email at *JMDFOIA@usdoj.gov*. The envelope and letter should be clearly marked "Privacy Act Access Request." The request should include a general description of the records sought, and must include the requester's full name, current address, and date and place of birth. The request must be signed and dated and either notarized or submitted under penalty of perjury. While no specific form is required, requesters may obtain a form (Form DOJ-361) for use in certification of identity from the FOIA/Privacy Act Mail Referral Unit, Justice Management Division, United States Department of Justice, 950 Pennsylvania Avenue N.W., Washington, DC 20530–0001, or from the Department's Web site at *http://www.justice.gov/oip/forms/cert_ind.pdf*. Some information may be exempt from the access provisions as described in the "EXEMPTIONS PROMULGATED FOR THE SYSTEM" paragraph, below. An

individual who is the subject of a record in this system may access any stored records that are not exempt from the access provisions. A determination whether a record may be accessed will be made at the time a request is received.

CONTESTING RECORD PROCEDURES:

Individuals seeking to contest or amend information maintained in the system should direct their requests to the address indicated in the "RECORD ACCESS PROCEDURES" section, above. The envelope and letter should be clearly marked "Privacy Act Amendment Request." The request must comply with 28 CFR § 16.46, and state clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought. Some information may be exempt from the amendment provisions as described in the "EXEMPTIONS PROMULGATED FOR THE SYSTEM" paragraph, below. An individual who is the subject of a record in this system may seek amendment of those records that are not exempt. A determination whether a record may be amended will be made at the time a request is received.

NOTIFICATION PROCEDURES:

Individuals may be notified if a record in this system of records pertains to them when the individuals request information utilizing the same procedures as those identified in the "RECORD ACCESS PROCEDURES" paragraph, above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

The Attorney General will promulgate regulations exempting this system of records from subsections (c)(3), (d), (e)(1), (e)(4)(G), (H), and (I) and (f) of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(k)(1) and (k)(2). These exemptions apply only to the extent that information in the system of records is subject to exemption, pursuant to 5 U.S.C. 552a(k)(1) and (k)(2). The Department is in the process of

promulgating regulations in accordance with the requirements of 5 U.S.C. 553(b), (c), and (e), that will be published in the Federal Register.

HISTORY:

64 FR 73,585 (Dec. 30, 1999): First published in full.

66 FR 8425 (Jan. 31, 2001): Modified to add a new routine use.

72 FR 3410 (Jan. 25, 2007): Modified to add a new routine use.

82 FR 24147 (May 25, 2017): Rescinded 72 FR 3410 (Jan. 25, 2007), and modified to add new routine uses.

[FR Doc. 2021-14986 Filed: 7/13/2021 8:45 am; Publication Date: 7/14/2021]